



A11103 761249

NISTIR 4816

REFERENCE

NIST
PUBLICATIONS

PBX Administrator's Security Standards

**Developed by the Federal
Deposit Insurance Corporation**

**Edward Roback
NIST Coordinator**

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

QC

100

.U56

4816

1992

NIST

PBX Administrator's Security Standards

**Developed by the Federal
Deposit Insurance Corporation**

**Edward Roback
NIST Coordinator**

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

April 1992



**U.S. DEPARTMENT OF COMMERCE
Barbara Hackman Franklin, Secretary**

**TECHNOLOGY ADMINISTRATION
Robert M. White, Under Secretary for Technology**

**NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director**

Preface

This National Institute of Standards and Technology Interagency Report (NISTIR) presents the Federal Deposit Insurance Corporation's (FDIC) PBX Administrator's Security Standards. It was developed to provide a generic set of security standards to phone system administrators and users throughout FDIC. The document discusses telephone policy, PBX fraud, PBX administration and anticipated future concerns. The duties and responsibilities for PBX system administrators may prove to be of particular interest to federal departments and agencies.

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of these standards. However, as this material may be of use to other organizations, it is being reprinted by NIST to provide for broad public dissemination of this federally sponsored work. This publication is part of a continuing effort to assist federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987.

NIST expresses its appreciation to FDIC for their kind permission to publish this report. We also wish to acknowledge the many security professionals who participated in the development of these standards, and in particular: Mr. Brian Seborg, Task Manager; Mr. Earl Bears, Chief, Voice Network Services Unit; Mr. Garrett Mussmann, Chief, Automation Security Unit; Mr. Gary Sarsfield, Chief, Branch Support Section; and Mr. John Laclede, I-NET Program Manager.

Questions regarding this publication should be addressed to the Associate Director for Computer Security, Computer Systems Laboratory, Building 225, Room B154, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA, 22161, telephone: (703) 487-4650.



PBX Administrator's Security Standards

Section 1: FDIC Telephone Policy

FDIC Telephone Usage Policy	1-1
PBX Protection Policy	1-1
Acquisition Policy	1-1
Security Incident Reporting Policy	1-1
Typical Telephone System Configurations	1-2
Terms Used in GS/SYS85 and G1/SYS75	1-3

Section 2: PBX Fraud

PBX Fraud History	2-1
Illegally Obtaining Authorization Codes	2-2
Observation	2-2
Social Engineering Schemes	2-2
Operator Direct Dial Scheme	2-2
Call/Sell Operations	2-3
Call Diverter Schemes	2-3
Remote Access Fraud	2-3
Voice Mail Fraud	2-4
Recent Telephone Industry Trends	2-5

Section 3: PBX Administration

Summary of Responsibilities	3-1
Duties and Responsibilities	3-3
Know Your PBX	3-3
Monitor PBX Options and Settings	3-3
Set Passwords	3-3
Review Telephone Bills	3-4
Educate Fellow Employees	3-5
Set Time and Day Restrictions	3-5
Destroy Old PBX Manuals	3-6
Protect Corporate Telephone Books	3-6
Know the Symptoms of PBX Fraud	3-6
Know the Symptoms of Voice Mail Fraud	3-7
Protect Your Voice Mail System	3-7
Restrict DID and Outward Calling Access	3-8
Prohibit DISA Use	3-9
Restrict Call Transfer Capabilities	3-10
Change System Administrator Passwords	3-11
Limit Country Code Access	3-12

Only Provide Services Required by the User 3-13

Protect Modem Pools 3-14

Restrict Direct Access to Trunks 3-15

Limit Incoming Call Capabilities 3-16

Use Networking Services Effectively 3-17

Physically Protect All Equipment 3-17

Security of Diskettes, Tapes, Backups
and other Computer Related Equipment 3-18

Ensure Physical Security of Shared Equipment 3-19

Secure Building Cable Plant Access Points 3-19

Apply PBX Security Measures to Key Telephone Systems 3-20

Maintain Up-to-Date Records of Configuration 3-20

Maintain Copies of Contractual Agreements 3-21

Make End Users Aware of Their Responsibilities 3-22

Summary of End User Responsibilities 3-23

Report All Security Incidents 3-24

Section 4: Future Concerns

Looking Toward the Future 4-1

Common Channel Signaling System 7 (CCSS7) 4-1

Appendix

Appendix: Terms and Definitions A-1

Section 1:
FDIC Telephone Policy

**FDIC Telephone
Usage Policy**

The use of FDIC long distance telephone service for any reason other than conducting official FDIC business is prohibited. Use of long distance service can be monitored. All FDIC PBX equipment has the capability of producing a list of long distance calls made from each extension.

**PBX Protection
Policy**

FDIC equipment shall be configured to prevent unscrupulous intruders from compromising our equipment, whether owned or leased. Telecommunication fraud is illegal in every state, and certain types of fraud are federal offenses as well. Unfortunately, when thieves use the FDIC's equipment to steal long distance service, the FDIC may be responsible for the costs incurred.

Acquisition Policy

All orders for voice communication services shall be placed by the Voice Network Services Unit (VNSU). If additional voice communication services are required, contact the VNSU.

**Security Incident
Reporting Policy**

Any security incident involving compromise of an FDIC PBX, voice messaging system, or associated equipment shall be immediately reported to the Voice Network Services Unit and the Automation Security Unit (ASU).

Report all telecommunications security incidents immediately to:

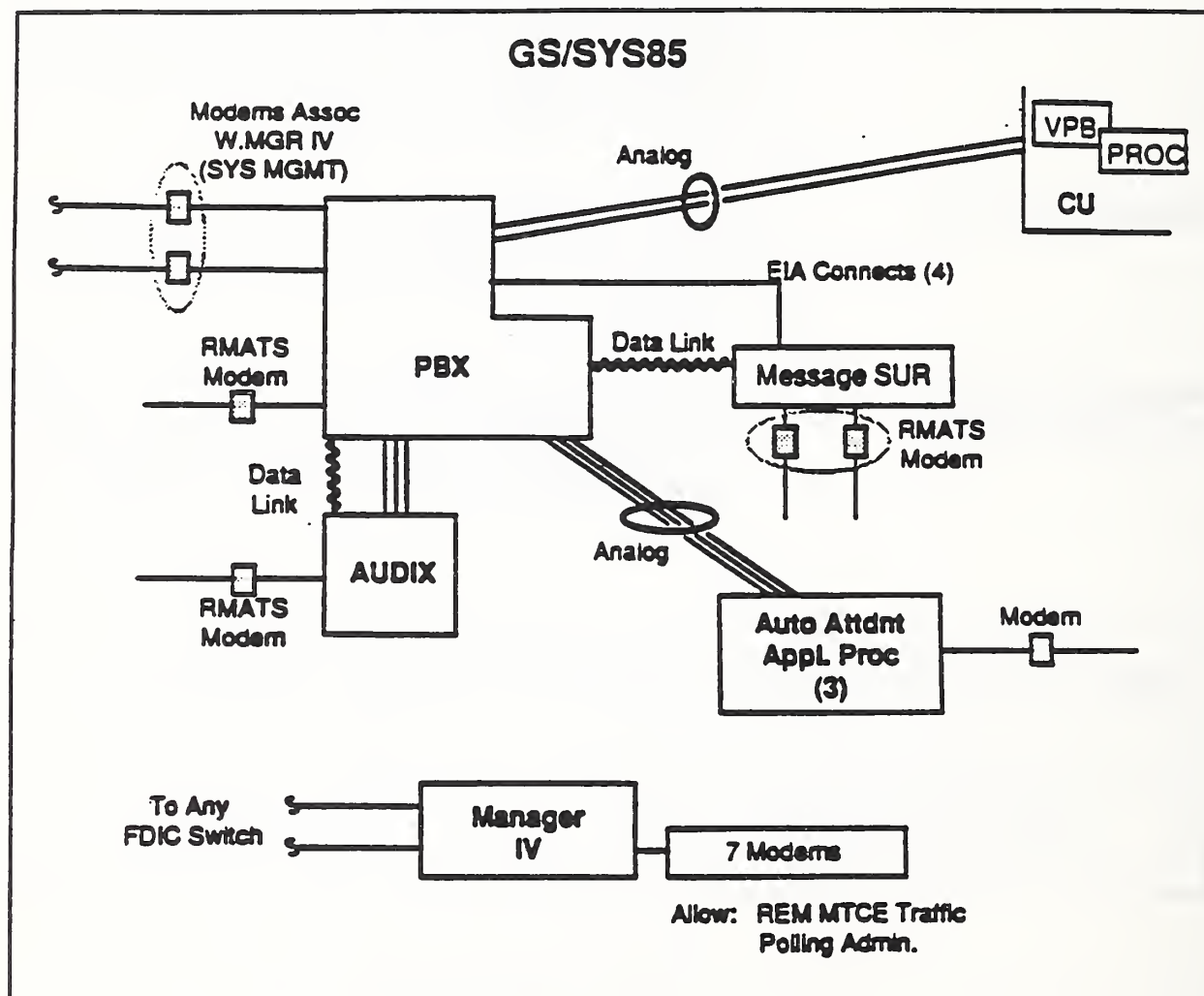
Chief, Voice Network Services Unit (703) 516-1108

Chief, Automation Security Unit (703) 516-1282

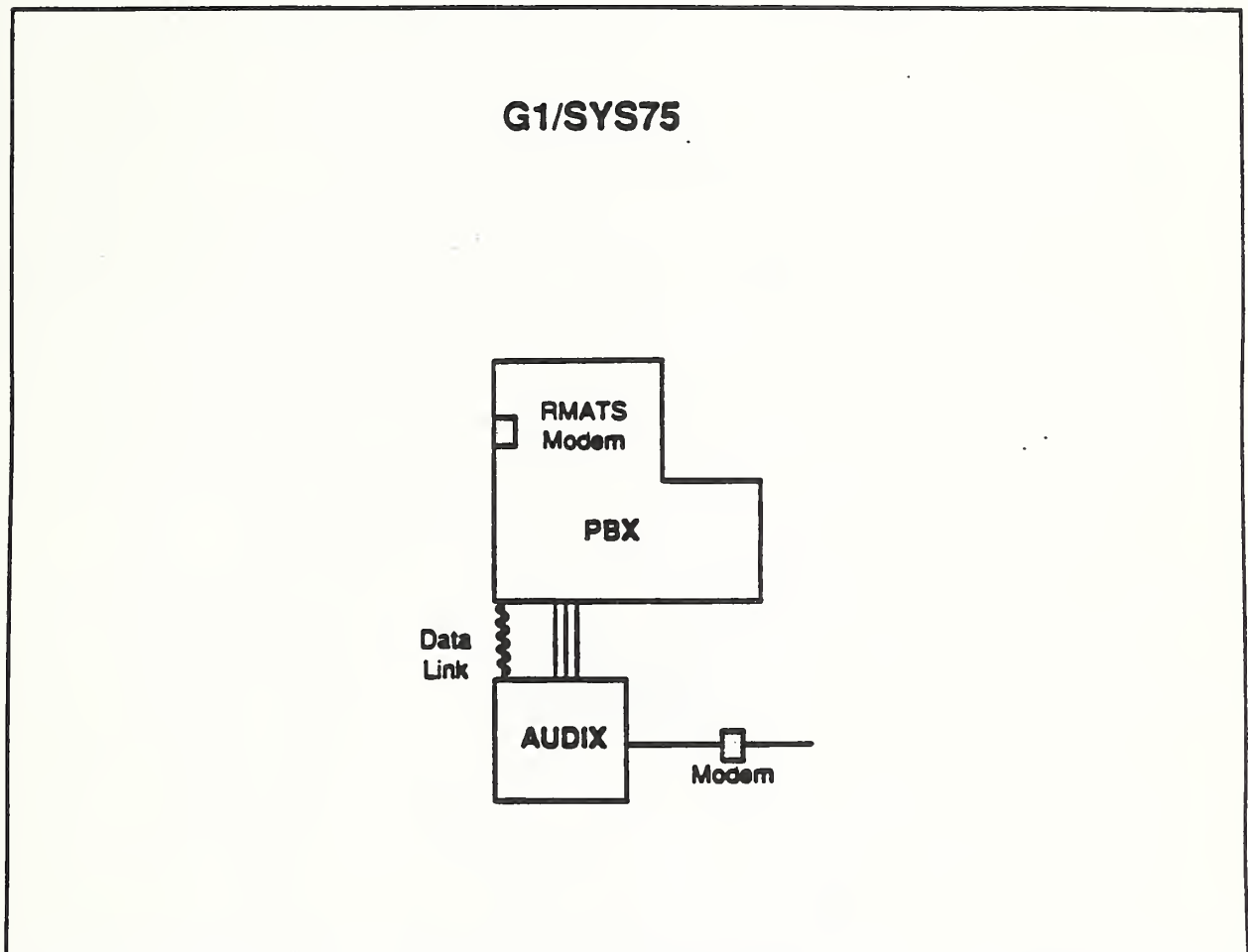
Typical Telephone System Configurations

In this manual security information is provided about your PBX and adjunct systems. Adjunct systems are processors, access devices, or any related piece of equipment that supports PBX or voice mail system operation, maintenance, or administration. The schematics included in this manual provide some background information on the interconnection of these pieces of equipment.

This figure shows a large scale telephone system operation, similar to the one at FDIC headquarters.



This figure shows a configuration similar to that used in most FDIC offices.



***Terms Used in
GS/SYS85 and
G1/SYS75***

<i>Analog</i>	Data in the form of a continuous variable signal (e.g., voice or light).
<i>Audix</i>	Audio Information Exchange.
<i>CU</i>	Control Unit.
<i>EIA</i>	Electronic Industries Association.
<i>Modem</i>	A device used to transmit and receive data.
<i>RMATS</i>	Remote Maintenance, Administration and Traffic System.

Section 2: PBX Fraud

PBX Fraud History

For as long as fees have been levied for making phone calls, there have existed thieves who have schemed to circumvent these charges, especially, long distance charges.

Long distance fraud existed prior to divestiture of AT&T, but it was less visible since the costs were simply passed on to the consumer. After divestiture the opportunity for fraud increased. In the beginning, long distance carriers were the primary victims of toll fraud. Toll fraud began with thieves breaking into the coin boxes of pay phones. Eventually, clever thieves who understood telephony developed tone generators, called blue and black boxes. These devices generated Single Frequency (SF) tones that told the long distance company's switch that the phone was still ringing and had not been answered, when in fact, it had. Next, third party billing (calls billed to a third party without the subscriber's consent) became a fraud avenue. Thieves who steal long distance calls refer to themselves as phreakers or phone hackers. While the terms are interchangeable, throughout this text we will use the term hacker, to refer to them.

Long distance companies entering the market initially relied on a five or six digit Personal Identification Number (PIN) to provide each customer access to their networks. Codes were easy to break and companies using them were very vulnerable. Long distance companies lengthened their codes to seven, nine and finally, to the 14-digit authentication codes currently used. Even 14 digit codes are vulnerable since the first ten digits are usually the home phone number and the last four digits are the PIN.

Hackers are no longer targeting the long distance carriers for toll fraud abuse. They are now looking to PBXs as prime targets for the following reasons:

- As long distance carriers got smarter about securing their networks, hackers began to look for

Illegally Obtaining Authorization Codes

Observation

easier ways to steal services. Hacking a 14 digit code is more difficult than hacking a PBX that is not securely administered.

- Long distance providers are no longer tolerating toll fraud. They have successfully prosecuted and jailed hackers caught breaking into their systems and stealing their services.

There are a variety of ways in which a hacker may illegally obtain someone's long distance authorization code. For example, hackers have been known to sit on balconies in busy airports or train stations overlooking telephone banks. Using telescopes or field glasses, they watch a traveler make a long distance call, and through careful observation, obtain the authorization code.

Social Engineering Schemes

Social engineering refers to a person's ability to use personality, knowledge of human nature, and social skills to steal toll calls. In one scheme, a hacker calls a long distance subscriber and claims to represent his/her long distance carrier. The hacker might claim to be doing maintenance or validating long distance access codes (PINs). He reads the first ten digits of the access code (which is the phone number of the person he is talking to) and makes up the last four digits. Human nature being what it is, the victim automatically corrects the hacker, giving him the correct PIN. The hacker thanks the subscriber and hangs up in full possession of a valid authorization code for placing long distance calls.

Operator Direct Dial Scheme

In this scheme, a thief employs his social engineering skills to convince a switchboard operator to assist him in placing a long distance call. Commonly, the thief dials your 800 number and asks for a particular department, such as Marketing. Once connected to that department, he says he has been connected to the wrong department and asks to be transferred back to the operator. When connected to the operator, the operator sees the call as originating internally because the thief was transferred to

Call/Sell Operations

the operator from an internal extension. The thief then asks the operator for help in dialing a long distance call.

A call/sell scheme is defined as the illegal sale, call-by-call, of the services of a compromised communications system. Once someone discovers a way to place long distance calls at someone else's expense, they set up shop with a cellular or pay phone and charge local residents or passers-by cut rates to make long distance calls. For example, a twenty minute call to the Dominican Republic might be sold for two dollars, payable in cash before the call is placed. Once paid, the hacker, using the compromised authorization code, dials the number for the user and hands the receiver to the person who bought the call. Call/sell operations are usually set up on street corners. If you have ever driven down a city street and seen people lined up by one pay phone while adjacent phones are being ignored, you have seen a call/sell operation in progress.

Call Diverter Schemes

Call diverters are becoming popular in the business community. They are used to forward calls to a remote location after normal business hours. For instance, a business with offices on the east and west coast may send calls from the east coast office to the west coast after the close of business to ensure important calls are not missed. The hacker dials the company's telephone number after hours to determine if the call is diverted to an operator, an answering machine, or a service. If the diverted call is answered by an operator, the intruder may attempt to convince the answering party that he/she has misdialed and needs an outside dial tone. A second possibility is that the intruder remains silent and waits for the called party to hang up. At this point, there may be a few seconds of dial tone which the hacker may take advantage of by speed dialing the desired number.

Remote Access Fraud

Most PBXs are capable of doing more than transferring calls and providing access to the Public Switched Telephone Network (PSTN). One PBX feature, known as remote access or Direct Inward System Access

(DISA), makes the PBX vulnerable to fraud. This feature allows a caller to dial into the PBX using a local or 800 number. The user then enters a combination of digits that serves as an access code to the outgoing telephone services used by the company, including domestic long distance, international long distance, and 900 service. The risk of allowing remote access is that the code will be discovered (that is, compromised) by a hacker, enabling fraudulent calls to be originated through the PBX. Once a code has been compromised, a hacker will use the local or 800 number to make a free call into the system, enter the access code, and dial the desired long distance telephone number. Hackers also share compromised code numbers through computer bulletin board systems allowing all their friends and fellow hackers to take advantage of the compromised code.

Voice Mail Fraud

A voice mail system is an unattended answering service that may be associated with a PBX. A voice mail system allows callers to leave messages in mailboxes for retrieval by voice mail subscribers. Some systems allow connection to outgoing PBX services as well. All voice mail systems provide some type of password security, usually in the form of a personal identification number (PIN).

Hackers will attempt to gain control of voice mailboxes to use the same voice messaging services enjoyed by legitimate system users. Hackers may, for example, use mailboxes as voice bulletin boards to make known lists of compromised calling card numbers, credit card numbers, etc., or to pass instructions on penetration techniques. Additionally, a compromised voice mail system that is configured to allow access to outgoing PBX services provides yet another means of stealing long distance service and of committing the full range of PBX fraud scams, such as call/sell operations.

A hacker normally gains access to a voice mailbox by dialing a local or 800 number and then, by trial and error, discovering the PINs associated with voice

Recent Telephone Industry Trends

mailboxes. For convenience, a common voice mail system administration technique is to use extension numbers as default PINs. Because uneducated users are not aware that these default PINs are easily hacked, they neglect to change these easily remembered numbers. Since PINs can be changed once access to the mailbox is gained, a hacker has the ability to change the PIN and to deny access to the authorized user of the mailbox. Having taken over the mailbox, the hacker may then use the voice mail service for his own convenience, and/or may pass the local or 800 number and stolen PIN to other hackers. There have, for example, been numerous instances where drug traffickers have used stolen voice mailboxes to pass messages to each other.

PBX administrators should be aware of recent trends in the telephone industry. The high growth period of the 80's has given way to a slow growing, and, in some cases, shrinking market for telephone service and equipment providers. As a result, many service and equipment providers have been forced to lay off highly capable and knowledgeable technical personnel. These technical personnel are intimately familiar with the workings of PBX and ancillary equipment. They are aware of the default login passwords, the avenues for attaching to PBXs, and the weaknesses of most PBX implementations. In some cases, these people are disgruntled individuals who wish to take adverse actions against their former employers. These people sometimes vent their frustrations on PBXs that do not have optimal security measures in place.

Section 3: PBX Administration

Summary of Responsibilities

The next page contains a summary of your responsibilities as a PBX Administrator. The pages that follow this *Summary of Responsibilities* provide more detail on each responsibility listed. You can easily look up more information on each by looking in the text for a bold, italicized version of the responsibility. The information that follows this formatted text explains more about the topic.

For each responsibility that has a specific associated requirement, such as a minimum password length or frequency of password change, a *Requirements* section has been included. Where no specific requirements are listed, the PBX Administrator is responsible for developing controls and procedures appropriate for his/her environment.

The PBX Security Administrator shall:

- Become knowledgeable about PBX and all adjunct system capabilities.
- Monitor all PBX and adjunct system options and settings periodically.
- Set all passwords to conform to FDIC requirements.
- Ensure that telephone bills and call detail reports are reviewed for fraud and abuse.
- Educate fellow employees about how to avoid PBX fraud.
- Determine appropriate time of day/day of week access restrictions.
- Shred and dispose of old PBX manuals.
- Protect corporate telephone books and directories from unauthorized access.
- Know the symptoms of PBX and voice mail fraud.
- Protect your voice mail system from unauthorized access.
- Restrict DID and outward calling access to stations with an operational requirement.
- Prohibit the use of Direct Inward System Access (DISA).
- Restrict call transfer capability to within the PBX for automated attendant systems.
- Enforce monthly change of PBX and adjunct system administration passwords.
- Block country code access where FDIC operations do not take place.
- Limit telephone service to that required by the station.
- Protect modem pools by using COS/COR restrictions.
- Restrict direct access to trunks and trunk groups.
- Restrict the ability of incoming calls to access outgoing trunks.
- Use FDIC's networking services to maximize calling efficiency and to minimize abuse.
- Ensure that PBX, adjunct system equipment, and wire closets are physically secure.
- Apply physical security measures to shared building or telephone facilities.
- Apply PBX security measures to key telephone systems, to the extent possible.
- Maintain up-to-date, complete configuration management records.
- Maintain copies of all contractual agreements for PBXs and PBX services.
- Ensure that end users are aware of their telephone system security responsibilities.
- Report all PBX related security incidents to the VNSU and ASU.

Duties and Responsibilities

Know Your PBX

Become knowledgeable about your PBX and all adjunct system capabilities. As the designated PBX Administrator at your location, you have numerous responsibilities. First and foremost, you must understand all the capabilities of your PBX and voice mail system. Obtain and read the current copies of your PBX and voice mail system manuals to develop an understanding of how these systems provide the services that this standard describes. PBX and voice mail system vendors frequently provide administrator training; talk to your supervisor about enrolling in these classes.

Monitor PBX Options and Settings

Monitor all PBX and adjunct system options and settings periodically. When your PBX was installed, a set of features was enabled. Through site records or conversations with your vendor, find out what options were purchased and installed with your PBX. Using remote maintenance capabilities, knowledgeable hackers may be able to log into your switch and change or enable feature functionality.

Requirement:

- Determine the normal settings for these features and periodically confirm that these settings have not mysteriously changed.

Set Passwords

Set all passwords to conform to FDIC requirements. As the PBX Administrator, you must ensure that all vendor-defined administration and maintenance passwords are changed. All PBXs of the same type are delivered with these same passwords! If a hacker familiar with PBX installation procedures gains access to your PBX software (either directly or remotely), he/she can log in to your PBX. Re-assign these passwords periodically. Passwords should be randomly assigned so they are not easily guessed. Avoid using the name of a spouse, child, or pet. The combination of two words or the intermix of alpha and numeric characters usually works best, since such combinations are difficult to guess. For access codes, avoid easily guessed patterns, such as 1234, and

obvious choices like a family member's date of birth, or your office building's street address. If more than one access code is required, avoid using a block of numbers, such as 7000 - 7999. If one of these numbers is guessed, so are all the rest.

Requirements:

- Use a minimum of eight (8) characters when creating a password.
- Use a combination of alpha and numeric characters or two concatenated unrelated words when creating a password.
- Change passwords once a month.

Review Telephone Bills

Ensure that telephone bills and call detail reports are reviewed for fraud and abuse. Review monthly bills from the phone company for calls that are out of the ordinary. Numerous calls to a 900 number may indicate telephone system abuse, while high volumes of 800 number calls may be indicative of fraudulent activities.

Your PBX has the ability to list outgoing and incoming calls for each station. These listings may be referred to as Call Detail Records (CDRs) or Station Message Detail Records (SMDRs). Discussions with your local management should determine how this information can best be used. Contact the VNSU for further information about handling and using this data.

When reviewing these records, look for these indicators of fraud or attempted fraud:

- Numerous inbound calls of a very short duration. These types of calls often indicate hackers are attempting to discover access codes.
- Outbound calls of long duration.

- A high volume of calls during off-peak hours.
- A high volume of calls to locations not typically called by your organization.
- An inordinately high volume of calls to any location.

Requirements:

- Review monthly telephone records for signs of telephone fraud.
- Retain this information in accordance with FDIC Circular 1210.1, FDIC Records Retention and Disposition Schedule.

Educate Fellow Employees

Educate fellow employees about PBX fraud. Alert your users to the techniques hackers have been known to use. In particular, make users aware of social engineering approaches. Any user with the ability to provide outgoing trunk access to another user should consider that the voice on the other end of the line may not be who or what he/she claims to be. That voice may belong to a hacker who is trying to access outgoing services, or to elicit information about your system that will lead to a theft of services.

Set Time and Day Restrictions

Determine appropriate time of day/day of week access restrictions. In safeguarding your system, it may be desirable to limit access to PBX and voice mail services outside normal business hours. Many PBXs provide ways to restrict evening and weekend telephone services. For example, a station could be totally unrestricted from 7:00 a.m. until 7:00 p.m., Monday through Friday, and be restricted to internal calls at all other times.

Destroy Old PBX Manuals

Shred and dispose of old PBX manuals. When you receive new PBX manuals, you should shred and dispose of the old ones. Hackers have been known to search through dumpsters (known as *dumpster diving*) looking for old manuals that provide information about the administration and maintenance of your PBX.

Protect Corporate Telephone Books

Protect corporate telephone books and directories from unauthorized access. Do not distribute copies of FDIC telephone books and directories to non-FDIC employees. Destroy old, unwanted copies of these documents. These phone listings provide hackers with information that they might otherwise have to guess, making their job of gaining illegal access into your system easier. Advise fellow employees about this policy.

Know the Symptoms of PBX Fraud

Know the symptoms of PBX fraud. As an administrator, you should be aware of the warning signs that may indicate you are the victim of fraud. Your telephone bills provide an excellent resource for monitoring possible abuse. As mentioned earlier, look for increases in 900 calls. Also, look for increases in outbound call activity that do not have a logical explanation. Investigate international calls; your location should have very few, if any. Look for calls placed to areas of the country you do not normally serve or do business with.

If your inbound 800 circuits suddenly become constantly overloaded, Hackers may have compromised your PBX through the 800 service for the purpose of making free outgoing long distance telephone calls. If you receive complaints that the 800 number is always busy, you should investigate this possible cause.

Your PBX provides a call monitoring capability that you may want to use to track down various forms of fraud. You may, for example, want to seek management approval to randomly monitor calls for foreign language conversations if you have observed a sudden increase in the volume of international calls. Since local, state and federal laws govern the use of this ability to eavesdrop on conversations, this feature shall not be used without obtaining prior permission from the Management Information Services Branch (MISB). For further information about using this option, contact MISB.

Know the Symptoms of Voice Mail Fraud

Know the symptoms of voice mail fraud. If your location is served by a voice mail system, some of the symptoms of fraud are the same as with your PBX. For instance, if inbound call volume increases without explanation, a problem may be indicated. One telling sign of a potential problem is that users or administrators are suddenly denied access to their voice mail accounts for no logical reason. Most voice mail systems limit the number of attempts a user can make to access the system before permanently being locked out. If a user hasn't made mistakes attempting to access the system and finds himself locked out, this may be symptomatic of a hacker attempting to gain access to the user's voice mail box.

If hackers take over a voice mail system, they may change all the access codes so that only they can use the system. Another symptom is when access codes are no longer required to use certain capabilities. This may indicate that a hacker has penetrated your system and changed the log-in requirements.

Protect Your Voice Mail System

Protect your voice mail system from unauthorized access. To protect your voice mail system, apply the same procedures as with your PBX in terms of assigning passwords and access codes.

Requirements:

- Use a minimum of eight (8) characters when creating a voice mail administrator password.
- Change the voice mail administrator passwords once a month.
- Use a minimum of four (4) characters when creating a voice mail user password.
- Change the voice mail user passwords every six months.

- Discourage users from using their extension number as their voice mail password.
- Check the system, periodically, to ensure that each mailbox has a valid password associated with it.
- Delete old mailboxes when users terminate or transfer from your organization.
- Do not enable mailboxes for unassigned extensions.

Restrict DID and Outward Calling Access

Restrict DID and outward calling access to only those stations with an operational requirement. DID is an optional service provided by your local exchange carrier (LEC). This service allows calls coming in from the Public Switched Telephone Network (PSTN) to be directly terminated at a specific telephone set, using a relatively small number of trunk circuits. A PBX serving 200 station users is typically equipped with 20 DID trunks connected to the serving Central Office (CO). Under control of the CO, any one of these trunk circuits may be used by the incoming PSTN caller for completion of a telephone call to a station connected to the PBX. With DID service, the caller is directly connected to the person being called. Without DID service, a specific termination point (most often an attendant console, but possibly a station) must be assigned to each incoming CO line connected to the PBX. This requires most incoming calls to be answered by an attendant who then extends the call to the desired PBX station.

Medium to large organizations often opt for the significantly more costly DID service for the following reasons:

- Attendant console traffic is minimized; therefore, a smaller operator staff is required.

- A more responsive and professional organizational image is projected when incoming callers can directly access the person they are calling.

As with many features that enhance service, DID trunks are inherently less secure than their alternatives. By opting for DID service, each PBX Administrator must understand that pathways to the PBX and voice messaging systems have been made available to anyone with a telephone. If DID service is available at your site, strict adherence to the security standards presented in this manual are absolutely necessary to protect your system.

Requirements:

- Review the necessity for incoming DID service to extensions associated with the following functions:
 - Administrative or maintenance access ports to the PBX or adjunct processors.
 - Automated attendant access ports.
 - Extensions assigned to modem pools. (See the section entitled *Protect Modem Pools* for additional information.)

Prohibit DISA Use

Prohibit the use of Direct Inward System Access (DISA). DISA (also referred to as Remote Access) is a feature that allows authorized users to make long-distance calls through a PBX from a remote location. Typically, users dial a local or 800 number to be auto-answered by the PBX. The user must then dial a DISA access code to obtain a PBX dial tone. The user may then gain access to all PBX services as if he/she were using a directly connected station on the system. This allows the individual the use of direct outward dialing trunks to complete calls that will be billable to the FDIC.

Telephone users who require off-site long distance calling capabilities should obtain long distance carrier calling cards. PBX Administrators should contact the Chief of the Voice Network Services Unit for assistance in obtaining these cards.

Requirements:

- Prohibit DISA access from being activated except for test purposes.
- Use the following precautions when the DISA is activated for testing purposes:
 - Activate the feature only for the duration of the test.
 - Make the access code at least eight (8) characters long.
 - Change the access code at the conclusion of the test session.
 - Deactivate the feature at the conclusion of the test.

Restrict Call Transfer Capabilities

Restrict call transfer capability to within the PBX for automated attendant systems. An automated attendant system (often a voice messaging system feature) provides unattended processing of incoming telephone calls. PBX Administrators must be aware that although these systems can greatly reduce the number of attendant-processed calls, they also offer an avenue for PBX fraud. If a hacker is able to gain access to outgoing PBX services, either directly or through an attendant, he/she may originate long distance calls that will be billable to the FDIC.

Change System Administrator Passwords

Enforce monthly change of PBX and voice mail system administration passwords. Remote access ports are used by vendors, manufacturers, and administrators to access the PBX system from remote locations for maintenance and administrative functions, such as moves, adds, and changes. Access to these password-protected ports is gained by dialing a directory number associated with an auto-answer modem.

Some systems may require additional passwords that define the level of access to the system's software. It may be desirable to construct an access scheme that limits access to sensitive administrative operations (Automatic Route Selection (ARS) tables, toll restriction tables, etc.) to a select group.

PBX administrators can use these access ports to perform maintenance and administrative functions from remote locations. While remote maintenance and administration is convenient and cost-effective, its inherent security vulnerabilities must be recognized. Remote access ports provide the hacker with the same set of capabilities available to the legitimate administrator.

Requirements:

- Change the log-in passwords for these remote access ports on the first day of each month.
- Create passwords that are at least eight characters in length and composed of a combination of alpha and numeric characters or two disassociated, concatenated words.
- Protect modems connected to these ports from unauthorized use. Coordinate modem protection with the VNSU.

Limit Country Code Access

Block country code access where FDIC operations do not take place. Certain countries show up over and over again as the receiving location of stolen long distance calls. These countries include Pakistan, Columbia, and the Dominican Republic. By reviewing your call detail reports, you may be able to identify countries to which long distance calling should be prohibited. Your PBX may include a feature that allows you to prevent outgoing calls to these countries. If these restricted country codes are dialed, the PBX intercepts the call and either produces a reorder tone or connects you to an attendant. Your long distance provider can also restrict dialing to designated areas for your account. Long distance calls may still be made, but operator assistance will be required.

The FDIC network has been blocked from making long distance telephone calls to some countries. The following table shows the countries that have been blocked. For additional information about country code blocking, contact the VNSU.

LONG DISTANCE SERVICE NOT PROVIDED

Albania	355	Caribbean Basin	809*	Gibraltar	350
Algeria	213	Columbia	57	Greece	30
Bangladesh	880	Dominican Republic	809*	Venezuela	58
Bulgaria	359	Ecuador	593	Yemen	967
Burkina Faso	226	Ghana	233		

*** Countries Included in the 809 Country Code**

Anguilla	British Virgin Islands	Mustique	St. Lucia
Antigua	Cayman Islands	Nevis	St. Vincent
Bahamas	Dominica	Palom Island	Turks & Caicos
Barbados	Grenada	Puerto Rico	Union Island
Bequia	Jamaica	St. Kitts	U.S. Virgin Islands
Bermuda	Montserrat		

***Only Provide Services
Required by the User******Limit telephone service to that required by the station.***

Class of Service (COS)/Class of Restriction (COR) provides administrative control of access to PBX and calling capabilities. COS/COR programming allows system administrators to distinguish between the types of service offered to station users. PBX features that would be assigned to a particular COS/COR might be DID capability, ARS access, call forwarding, or automatic callback.

All PBXs provide you with the ability to build a number of user classes. The COS feature on PBXs is normally a numeric designation. For example, COS 4 might be used to specify a group of features accessible by a group of extension numbers or tie trunks. PBX administrators should use the COS feature to control extensions located in public areas such as cafeterias, reception areas, or photocopy centers.

The PBX toll restriction feature allows a system administrator to prevent station users from dialing specific strings of digits on each group of CO or tie trunks. With many systems, it is possible to monitor up to 14 user-dialed digits prior to determining whether to allow or deny completion of a particular telephone call. The most basic toll restriction schemes will generally allow monitoring of "1+" and Number Plan Area (NPA) code dialing.

PBX administrators must ensure that station users are permitted to only complete calls necessary for the performance of day-to-day responsibilities.

Protect Modem Pools

Protect modem pools by using COS/COR restrictions.

Rather than having a modem attached to a PC for one individual's use, modem pooling allows a group of users to share a bank of modems. Typically, a ten user to one modem contention ratio is acceptable. Modem pooling is accomplished through the association of a circuit pack in a PBX equipment shelf and a bank of external modems. The benefits of this feature must be carefully weighed against its inherent risks.

A hacker may exploit a PBX modem pool by first gaining access to the PBX or voice mail system, as previously described. He/she would then access a modem by dial access code, "dial by name" or by persuading the attendant to whom he/she is routed that he/she has misdialed and requires access to the modem pool. Once access to the pool is gained, the hacker may originate data calls that will be billable to the FDIC.

Requirements:

- Use Class of Service/Class of Restriction features of your PBX to protect your modem pool. If your PBX does not allow the use of such features with a modem pool, do not use modem pooling. Contact the VNSU for further information.
- Restrict service of modem pools to that required (that is, outbound only or inbound only).

Restrict Direct Access to Trunks***Restrict direct access to trunks and trunk groups.***

Programmable ARS tables within a PBX establish the primary and alternate routes for each combination of digits that can be dialed over each CO or tie trunk. Call routing may vary for different station user classes. Some PBX's allow time-of-day and/or day-of-week schedules that affect the routing of some or all calls. By allowing most station users to dial only the ARS access digit for the purpose of initiating outgoing calls, the PBX Administrator ensures that calls will be routed over the most economical, or otherwise desirable trunk or trunk group. The ability to directly access particular trunks or trunk groups should, in most cases, be reserved for the Security Administrator, the attendant console operators, and the telecommunications maintenance personnel.

When a user dials 9 to place an outside call, the call is routed over a randomly selected trunk. Dial Access Codes (DACs) are used to allow access to a specific trunk, such as a WATS (Wide Area Telecommunication Services) trunk. DACs should not be provided to the user except for paging trunks. Trunk group DACs shall be no less than 3 digits in length. DACs should be disabled except for testing purposes.

Requirements:

- Access to user trunks should be through ARS only.
- Use the following precautions if DACs are activated for testing purposes:
 - Activate the feature only for the duration of the test.
 - Make the code a three digit number.
 - Change the code at the conclusion of the test session.
 - Deactivate the feature at the conclusion of the test.

Limit Incoming Call Capabilities

Restrict the ability of incoming calls to access outgoing trunks. Tie trunks (also referred to as "tie lines") are normally used to connect two PBX's over leased digital or analog private lines. By keying the assigned ARS access code and the digits to be dialed, or by dialing the trunk group access code, the user on one PBX can assume the functionality of a station on the remote system. While this can be a convenient and cost-effective alternative to communication through the Public Switched Telephone Network (PSTN), PBX Administrators of the two systems must be aware that:

- If not restricted, incoming tie line callers may use PBX services as would any internal station.
- Unless some form of tie line reconciliation is provided, the call detail information on an outgoing call originated by the incoming tie line caller will not include the remote originating station.

In most cases, the Security Administrators of PBXs equipped with tie lines should ensure that no outgoing CO trunk access is permitted for incoming tie line callers. Incoming tie line caller access to outgoing tie trunk groups should be carefully reviewed because network security is dependent upon consistent treatment of each node in the network.

Use Networking Services Effectively

Use FDIC's networking services to maximize calling efficiency and to minimize abuse. FDIC uses networks provided by long distance companies. These networks provide improved service and lower cost to the Corporation. These services must be used to preserve FDIC's network security. Special service requests for specific locations shall be coordinated through the VNSU.

Physically Protect All Equipment

Ensure that PBX, attendant consoles, adjunct system equipment, and wire closets are physically secure.

Anyone who can physically access your PBX may be able to change settings, to make unauthorized calls, or to otherwise tamper with your system. Your PBX should be in a physically controlled area with access permitted to authorized personnel only.

Any room that contains equipment associated with the network (such as the PBX, attendant consoles, and adjunct system equipment) must be secured.

- Attendant consoles are powerful terminal devices that provide unrestricted access to all PBX trunks, thereby providing unauthorized users access to unlimited calling.
- An adjunct processor or access device is any piece of equipment that supports PBX or voice mail system operation, maintenance, or administration. Examples of such devices include maintenance terminals or other equipment that allows for the programming of multiple switches, such as the AT&T 3B2.

A card reader is preferred for securing this equipment, but if card reader access is not possible at your location, a cipher lock or key lock may be used. All telephone closets that contain wiring must be locked at all times. For exceptions to these requirements, contact the Automation Security Unit.

In addition to physical access control, the room where the PBX is stored should also be climate controlled. PBXs are sensitive electronic equipment that have specific environmental requirements. Just as computers have climate controlled rooms, so should PBXs.

The PBX room itself should be kept neat and free of old equipment, wire, paper, or trash. A messy room may lead to mishaps such as accidentally kicking out the PBX plug and causing phone service outage. Your PBX should have some type of backup power supply to allow for graceful management of the shutdown of PBX services in case of power outages or power inconsistencies.

You should also be aware of the equipment layout and density in your PBX room. If the PBX room is packed with heat producing equipment, it may be difficult to provide the proper climate controls. Equipment should be laid out to maximize space and safety.

Requirements:

- Keep all PBX and adjunct equipment in a locked room. While a card reader is the preferable locking mechanism, a cipher lock or key lock may be used instead.
- Make sure the access codes and/or passwords to any adjunct processor are eight characters long and changed monthly.

***Security of Diskettes,
Tapes, Backups and
other Computer-related
Equipment***

Subject the PBX, the voice mail system, and any adjunct systems to the same security requirements as other computer systems in use by the FDIC. In addition to maintaining access code and password security for this equipment, the PBX Security Administrator is responsible for maintaining the security of all system and data disks used by the system.

Ensure Physical Security of Shared Equipment

Requirements:

- Label and date all disks.
- Make backups of system data and store them in a secure location. An off-site location is preferable.

Ensure physical security measures to shared building or telephone facilities are used. Administrators who share a building and telephone facilities with other tenants have unique security concerns. Administrators must work with building management representatives to ensure physical security of the telephone facility and proper security of the shared PBX. In instances where a shared PBX is used, FDIC should be afforded the same security measures it would implement if the FDIC was not sharing the PBX. Work with building management to ensure the PBX room and all wiring closets are adequately secured.

Secure Building Cable Plant Access Points

Be concerned with the physical security of the building's cable plant. In most cases, Local Exchange Carrier (LEC) lines enter the building at the same physical location, regardless of who is using the lines. Usually the point of entry into the building is a room located in the basement of the building. Whether or not you share a building and telephone facilities with another company, you need to be concerned about the physical security of this room.

Requirement:

- Find out where this room is located and make sure that it is locked at all times.
- Work with building management, if this room is not locked, to obtain a lock and periodically check that it remains locked.

Apply PBX Security Measures to Key Telephone Systems

Apply PBX security measures to key telephone systems, to the extent possible. Although not as advanced as digital PBX systems, 1A2 and electronic key systems provide basic telephone services and must be secured. Basic electronic key systems cannot be remotely accessed, so there is no opportunity for hacking. However, good physical security practices are important because anyone who can physically access a key set can make unauthorized long distance calls. Some electronic key systems provide basic security features, such as call blocking and/or Station Message Detail Recording (SMDR). If you have a key system, find out what security features it has, and implement them to the same extent you would on a PBX.

Maintain Up-to-Date Records of Configuration

Maintain up-to-date, complete configuration management records. This is important to both the physical security and the successful management of PBX services to actively maintain an inventory of PBX equipment, and the cables, lines, and other auxiliary equipment that may be attached to it.

Requirements:

To maintain good configuration records:

- Check the number of lines installed against the number of lines you are billed for each month and resolve all inconsistencies.
- Keep records of all major wiring upgrades.
- Keep records of where spare pairs are located. Spare pairs are additional telephone wires that have been pulled to a location, but are not currently in use. You never know when you might need them during an emergency installation.
- Maintain an inventory of the number of extensions installed, and, to the extent possible, who they are assigned to.
- Maintain a coherent numbering plan. Certain blocks of numbers may be assigned to certain organizational elements. Know what they are, know how many numbers have been assigned and how many are unassigned.
- Keep track of the equipment and software version numbers.
- Notify VNSU before acquiring voice communications services.

Maintain Copies of Contractual Agreements

Maintain copies of all contractual agreements for PBXs and PBX services. If you currently have contractual agreements with telecommunications service providers for a PBX or PBX services, make sure you have a copy of the contract on hand. If you are planning to contract out for these services, you must notify the VNSU before entering into a contractual agreement for these services. Very often, telecommunications service providers try to

contractually limit their liability for unauthorized system access or theft of service. The VNSU will help you in ensuring that the FDIC is appropriately protected in these contracts.

Requirements:

- Maintain a file copy of all current telecommunications contracts.
- Notify VNSU before entering into new contracts or renewing existing ones.

***Make End Users Aware
of Their Responsibilities***

Ensure that end users are aware of their telephone system security responsibilities. As the PBX Security Administrator, you are responsible for ensuring that users of the PBX and voice mail systems under your control are required to maintain certain security standards. These standards include:

- Not divulging system access codes or passwords to anyone.
- Not sharing telephone long distance calling card access codes with anyone.
- Periodically changing voice mail passwords.

The following page contains a summary of responsibilities for end users. Copy this page and share it with your end users so that they are familiar with their responsibilities for PBX and voice mail security.

PBX and Voice Mail System Users shall:

- Use telephones and telephone services provided by the FDIC for business purposes only.
- Be alert to social engineering scams. Be suspicious of callers asking you for passwords or access codes for maintenance or any other purpose.
- Notify the PBX Security Administrator immediately if you suspect your telephone services or voice mail services are being used for fraudulent purposes.
- Report voice mail problems to the PBX Security Administrator immediately.
- Maintain as secret all system passwords and access codes.
- Maintain as secret long distance calling card access codes.
- Ensure that your voice mail password is at least four (4) characters in length.
- Change your voice mail system password every six months.

Report All Security Incidents

Report all PBX related security incidents to the VNSU and ASU. It is important that both the Voice Network Services Unit and the Automation Security Unit be notified immediately of any telecommunications security incidents. Through the use of a centralized reporting facility, lessons learned from a vulnerability discovered in one location can be applied to all FDIC locations.

Requirement:

- Report all PBX related security incidents immediately to:

Chief, Voice Network Services (703) 516-1108
Chief, Automation Security (703) 516-1282

Section 4: Future Concerns

Looking Toward the Future

Common Channel Signaling System 7

Over time, security measures are put into place to close existing gaps at just about the same time that new technology is being implemented. This new technology, no matter how carefully thought out, usually provides new avenues for hackers to explore. This section takes a look at some of the technology on the horizon and how it may impact PBX switch administration.

Common Channel Signaling System 7 (CCSS7) is the North American implementation of the International Telegraph and Telephone Consultative Committee's (CCITT) CCSS7. This is a common channel signaling protocol being adopted world-wide. This protocol defines the basic communications support required for advanced telephony services. It is a telephony oriented packet switching system that will provide:

- Exchange of trunk signaling information between switches using data links instead of on an in-band, per-trunk basis.
- The ability to exchange large amounts of data between switches and centralized databases with a high degree of reliability.

CCSS7 has several benefits:

- Improved network efficiency and economy.
- It provides a vehicle for real-time network management controls.
- Data and signaling transmissions travel over separate paths leaving no chance for mutual interference.
- Call set-up time is generally faster because signaling is faster.

CCSS7 has already been implemented by long distance carriers. In the early 1990s, the long distance providers

and the local exchange carrier (LECs) will integrate CCSS7 services. Following this move, CCSS7 will be implemented at the PBX level. When this happens, the PBX will have more capabilities and more intelligence. As a result, the PBX will become an even more attractive target for phreakers/hackers.

Appendix

Blue/Black Box

A device that generates a 2600 hertz tone. Under normal circumstances, the phone company's switch generates this tone to indicate that the receiving phone has not been answered and is still ringing. The switch allows the ring to occur indefinitely. Hackers use this device to generate this tone when the call has actually been connected. Since the switch does not start billing for calls until after they are answered, the blue/black box allows the hacker to talk without being billed. Most modern switches have changed the use of the 2600 hertz tone to eliminate this vulnerability.

Busy Signal

An audible signal (usually 60 pulses per minute) that indicates the called number is unavailable. A fast busy signal (120 pulses per minute) indicates all voice paths are temporarily unavailable.

Central Office (CO)

The location of the Local Exchange Carrier's switching equipment that services an area. A CO is the first connection the customer gets. For long distance service, the CO passes the call to a long distance provider. Each CO has its own exchange number. The exchange number is the first three digits following the area code.

Class of Service/Class of Restriction

The categorization of telephone subscribers according to specific type of telephone usage. Telephone service distinctions include rate differences between individual and party lines, flat rate and message rate, and restricted and extended area service.

Dial Tone

A 90 hertz signal sent to an operator or subscriber indicating that the receiving end is ready to receive dial pulses.

Local Exchange Carrier (LEC)

The telephone company that provides local service. For example, C & P is an LEC. Local Exchange Carriers control Local Access Transport Areas (LATAs).

<i>Private Branch Exchange (PBX)</i>	A private automatic exchange, either automatic or attendant-operated, serving extensions in an organization and providing transmission of calls to and from the public telephone network.
<i>Signaling</i>	The process by which a caller on the transmitting end of a line informs the party at the receiving end that a message is to be communicated. Signaling also includes supervisory information such as letting callers know that called parties are ready to talk, that the line is busy, or that either party has hung up. Signaling also holds the voice path together for the duration of the telephone call.
<i>Trunk</i>	A communication channel connecting two switching centers, or a switching center with an individual terminal. A trunk can also be a communication channel between two offices or between equipment in the same office. A trunk is used commonly for all calls of the same class that are generated between two terminals.
<i>Tie Trunk</i>	A trunk directly connecting two Private Branch Exchanges.
<i>Transmission</i>	The sending and receiving of signals from point A to point B while maintaining integrity of the information.

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER

NISTIR 4816

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE

April 1992

4. TITLE AND SUBTITLE

Federal Deposit Insurance Corporation's
PBX Administrator's Security Standards

5. AUTHOR(S) Recognition: Brian Seborg, Task Manager; Earl Bears, Chief, Voice Network Services Unit; Garrett Mussmann, Chief, Automation Security Unit; Gary Sarsfield, Chief, Branch Support Section; and John Laclede, I-NET Program Manager

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED

NISTIR

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

Reprinted by permission of the Federal Deposit Insurance Corporation, Washington, DC 20429

10. SUPPLEMENTARY NOTES

☐ DOCUMENT DESCRIBES A COMPUTER PROGRAM; SF-185, FIPS SOFTWARE SUMMARY, IS ATTACHED.

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

This NISTIR, PBX Administrator's Security Standards presents the Federal Deposit Insurance Corporation's (FDIC) generic security standards for phone system administrators and users throughout FDIC. It describes FDIC telephone policies, including those for system use, protection and acquisition. The history and current methods of PBX fraud are then presented. PBX Administration is considered in some detail, with a review of the duties and responsibilities of system administrations. These include: monitoring PBX options, setting passwords, educating users, reviewing billing records, protecting voice mail and limiting outgoing international calls. The Appendix consists of a brief list of terms and definitions used throughout the document.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

computer security; PBX security; private branch exchange security; telecommunications security; telephone fraud; telephone security

13. AVAILABILITY

☒

UNLIMITED

☐

FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

☐

ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE,
WASHINGTON, DC 20402.

☒

ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES

48

15. PRICE

A03

